IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

ONSITE HEALTH DIAGNOSTICS, LLC Plaintiff, v. AMERICAN CASUALTY COMPANY OF READING, PA, and COLUMBIA CASUALTY COMPANY Defendants.	§ § § § § § § § § §	Cause No.

PLAINTIFF'S ORIGINAL COMPLAINT

AND NOW comes Plaintiff Onsite Health Diagnostics, LLC, by and through its undersigned counsel, and brings this action to obtain damages, declaratory relief, attorneys' fees, and interests as allowed by law:

PARTIES

1. Plaintiff Onsite Health Diagnostics, LLC ("Onsite") is a Texas limited liability company, with its principal place of business at 1199 S. Beltline Road, Suite 120, Coppell, Texas 75019.

2. The LLC members of Onsite are as follows: (a) Kyle Alexander, who is a resident of Irving, Texas; (b) Richard D'Antoni, who is a resident of Irving, Texas; (c) Stephen K. Fannon, who is a resident of Irving, Texas; (d) Anthony Gibson, who is a resident of Flower Mound, Texas; (e) Michael Quinn, who is a resident of McLean, Virginia; (f) Marshall Watson, who is a resident of Fort Lauderdale, Florida; and (g) Soitis, LLC, which is an Indiana limited liability company, whose members in turn are Tony Robertson (a resident of Indiana) and Steve Staneff (a resident of Texas).

3. Defendant American Casualty Company of Reading, PA ("American Casualty") is a Pennsylvania corporation, with its principal place of business located at 333 South Wabash Avenue, Chicago, Illinois 60604. American Casualty issued a policy of insurance at issue in this lawsuit.

4. Pursuant to Federal Rule of Civil Procedure 4(h)(1), American Casualty may be served through its registered agent for service of process: CT Corporation System, 1999 Bryan Street, Suite 900, Dallas Texas 75201-3136.

5. Defendant Columbia Casualty Company ("Columbia Casualty") is an Illinois corporation, with its principal place of business located at 333 South Wabash Avenue, Chicago, Illinois 60604. Columbia Casualty also issued policies of insurance at issue in this lawsuit.

6. Pursuant to the terms of Columbia Casualty's insurance policies, and Texas Insurance Code section § 804.106—which are incorporated through Federal Rule of Civil Procedure 4(h)(1)—Columbia Casualty may be served through the Texas Secretary of State, with copies thereafter mailed to "General Counsel, Columbia Casualty Company, 333 S. Wabash Ave., Chicago, IL 60604."

NATURE OF ACTION

7. Defendant American Casualty and Defendant Columbia Casualty have breached their respective contractual duties of indemnification and violated statutory insurance "Settlement Practices" mandated by Texas Insurance Code Chapter 542.

8. As described herein, Onsite's computer network was breached in or about March 2014 due to a "vulnerability" in the network (the "Data Breach").

9. As a result of the Data Breach, one or more unauthorized persons were able to access and steal a significant volume of electronic records Onsite amassed to provide "health screening services" to its customers and third persons.

10. Onsite in turn was obligated to remedy the harm after being prompted by written requests by affected or potentially affected persons demanding Onsite mitigate the data theft, which was jeopardizing the customers and third persons.

11. Losses of the kind are covered by a contract of insurance issued by Defendant American Casualty. The policy is designated "Network Security, Privacy & Identity Theft Liability Policy" No. 4031611691 (the "NetProtect Policy"), attached hereto as **Exhibit A**.

12. Losses of the kind independently are covered by two contracts of insurance issued by Defendant Columbia Casualty.

13. The primary policy is designated "Healthcare Facilities Professional Liability Coverage Form – Claims Made" Policy No. HMA 4031930279-2 (the "Professional Liability Policy"), attached hereto as **Exhibit B**.

14. Columbia Casualty also provided "umbrella" coverage pursuant to a policy designated "Healthcare Facilities Umbrella" Policy No. HMC 4031936700-2 (the "Umbrella Policy"), attached hereto as **Exhibit C**.

15. Defendant American Casualty and Defendant Columbia Casualty nonetheless have refused, without cause, to fully indemnify Onsite's damages covered by the NetProtect Policy, Professional Liability Policy, and Umbrella Policy (when referenced collectively, the "Insurance Policies.").

16. American Casualty likewise failed to, *inter alia*, timely acknowledge receipt of Onsite's claim for coverage under the NetProtect Policy; timely investigate or evaluate the claim; or promptly resolve and pay losses covered by the NetProtect Policy—all as required by Chapter 542 of the Texas Insurance Code.

17. Columbia Casualty in its own right violated Chapter 542 by failing to, *inter alia*, promptly, fairly, and equitably resolve and pay Onsite's losses covered by the Professional Liability Policy and (as necessary) the Umbrella Policy.

18. Onsite therefore seeks to recover as follows to remedy American Casualty's and Columbia Casualty's contractual breaches and statutory violations: (a) breach of contract damages; (b) declarations regarding Onsite's rights and remedies under the Insurance Policies; (c) statutory damages recoverable under Chapter 542 of the Texas Insurance Code, or as otherwise allowed by law; (d) litigation attorneys' fees recoverable under Chapter 542 of the Texas Insurance Code, or as otherwise allowed by law; (e) pre-judgment and post-judgment interest recoverable under Chapter 542 of the Texas Insurance Code, or as otherwise allowed by law; and (f) all other relief to which Onsite is entitled.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(a), because Onsite (through its members) is a citizen of Florida, Indiana, Texas, and Virginia, whereas Defendants either are citizens of Pennsylvania or Illinois. There consequentially is complete diversity of citizenship between the parties, and the amount in controversy exceeds $75,000.00, exclusive of interest and costs.

20. The Court has personal jurisdiction over Defendants, because this dispute arises out of the construction, application, and enforcement of contracts of insurance issued by Defendants to a Texas-based insured; is based on Defendants' authorization to issue policies of the kind by the Texas Department of Insurance or other authority to transact business in Texas; and relates to professional services and electronic data maintenance that Onsite facilitated from its Texas-based operations.

21. Venue is proper in the Northern District of Texas pursuant to 28 U.S.C. § 1391(b)(2), because at the time of the March 2014 Data Breach, Onsite's services and the corresponding network data infrastructure were facilitated through Onsite's corporate headquarters in Irving, Texas, which is within this District, and Onsite now is based in Coppell, Texas, which likewise is within this District.

22. Venue otherwise is proper in the Northern District of Texas pursuant to 28 U.S.C. § 1391(b)(3), because Defendants are subject to personal jurisdiction in this District for reasons pleaded herein.

APPLICABLE LAW

23. The Insurance Policies were written to provide coverage for the benefit of Onsite as a Texas-based insured, based on American Casualty's authorization by the Texas Department of Insurance to issue a policy of the kind and Columbia Casualty's authority to transact business in Texas as a "surplus" lines insurer.

24. The respective policies further incorporate Texas law and were triggered by the professional services and related Data Breach that caused injuries to Onsite's Texas-based operations.

25. Texas law therefore applies to the claims at issue.

CONDITIONS PRECEDENT

26. Onsite has performed all conditions precedent to suit, including, but not necessarily limited to, providing Defendants with notices of claims and supporting documentation, and exhausting any applicable deductibles or self-insured retentions.

FACTUAL AVERMENTS

A. Onsite's Business

27. Onsite is a health screening vendor that provides health and wellness evaluations to employees of client companies.

28. Onsite generally does so either by contracting directly with employer companies or with those companies' health insurers.

29. Onsite also may contract with third-party wellness providers as part of the third-party providers' wellness programs.

30. In all such respects, Onsite collects personal information from screening participants, including, but not necessarily limited to, a given participant's name, date of birth, preferred mailing address, and email address.

31. Onsite also collects health-related information, including, but not necessarily limited to, height, weight, blood pressure, and cholesterol levels.

32. The foregoing information collectively shall be referred to as "Personal Data" or "Data" for all purposes herein.

33. The Personal Data was collected by Onsite to enable its client employers or health insurers to provide laboratory sampling results to the screening participants for diagnostic, preventative, assessment, and healthcare treatment uses—or to aggregate Personal Data in other was to provide health-related assessments.

34. A central requirement of Onsite's business operations therefore necessitated it organize, manage, direct, and control access to the Personal Data amassed during the screenings.

35. Onsite did so by storing the Personal Data in internet-accessible servers, hosted by Amazon Web Services.

36. It utilized two storage databases to maintain and control access to Personal Data relevant to this lawsuit.

37. Historically, it used a legacy system commonly referred to as "Original Scheduler," with a corollary system referred to as "Backup Scheduler."

38. In the normal course of business, Onsite also brought online a new system in or about January 2013, to maintain more current Personal Data amassed from screening participants. The new system herein shall be referred to as "New Scheduler."

39. Prior to the Data Breach, it was Onsite's practice to retain Personal Data for certain historical or long-running customers and third persons on Original Scheduler and Backup Scheduler.

40. Onsite had not prior to the Data Breach migrated that Data to New Scheduler.

B. Onsite's Legal Duties Regarding Personal Data

41. Onsite's customers, whether employers, insurance companies, or wellness providers, each signed Master Services Agreements ("MSAs"), which outlined the respective parties' rights and obligations regarding Onsite's health screening services.

42. As an Addendum to the MSAs, Onsite often executed a Business Associate Agreement ("BAA"), as required by the Health Insurance Portability and Accountability Act.

43. Apart from independent duties that arose by law to safeguard the Personal Data, Onsite's MSAs and BAAs generally required Onsite to: (a) notify a customer of a security breach or security incident; (b) pay for or compensate the customer for mitigation required as a result of any such breach; and (c) cooperate in any related investigation, whether by a state or federal agency.

44. Onsite's MSAs also required Onsite to obtain and maintain insurance coverage for a variety of potential events, in some instances including network security breaches.

C. The March 2014 Data Breach

45. Although at the time unbeknownst to Onsite, in or about March 2014, an unauthorized person or persons targeted a vulnerability in Onsite's computer network to surreptitiously access, then steal, Personal Data that had been stored on the Original Scheduler and Backup Scheduler.

46. A later-commissioned forensics analysis by the security firm Stroz Friedberg, dated June 2, 2014 (the "Stroz Report"), diagnosed the Data Breach as follows:

> The evidence demonstrates that both the Original Scheduler server and [a] Backup Scheduler server were compromised. The attack vector for the compromise was a *vulnerability* in, and exploit of, the Apache Struts Java Framework ("Struts") that was in use on the [Onsite] servers[.] This *vulnerability* allowed the attacker(s) to initiate commands remotely on the servers. . . .
>
> Early in the morning on March 25, 2014, the attacker(s) targeted the Scheduler database. Stroz finds strong evidence to suggest that the 'user' table in the Scheduler Database was targeted *and downloaded* by the attacker(s).
>
> . . . . [B]ased on the analysis set forth below, Stroz identified evidence that shows the attacker specifically compromised the Scheduler Database.

Exhibit D attached hereto (emphasis added).

47. Although not confirmed or diagnosed until Onsite received the Stroz Report in June 2014, Onsite first was cautioned about the possibility of the Data Breach by a series of customer communications than began in April 2014.

D. Client Demands for Remedies

48. As of April 2014, grocery retailer "Safeway" was an Onsite customer who had contracted for Onsite to provide healthcare screenings to Safeway's employees.

49. Corporations such as Safeway sometimes are targeted by cyber criminals, who attempt to penetrate the corporation's computer networks, and if successful, download personal information stored thereon—then market the surreptitiously obtained information (often personnel related) through "underground" internet forums.

50. Aware of that general risk, in or about April 2014, Safeway utilized the internet security firm iSight Partners ("iSight") to monitor activity within certain internet forums to assess whether sensitive Safeway data perhaps may have been compromised by a surreptitious network penetration.

51. On or about April 10, 2014, iSight concluded data associated with Safeway's employees indeed was being marketed in an underground internet forum—but iSight did not believe Safeway's network was the source of a network breach whereby the data was stolen.

52. iSight instead believed the information corresponded with the type of Personal Data Onsite had been amassing during health screenings—which thereafter was stored on Onsite's network as an extension of those services.

53. Safeway representatives therefore E-mailed Onsite regarding the suspected "Security Breach" on April 11, 2014—attaching the iSight report and requesting Onsite confirm whether a breach had occurred. *See* **Exhibits E, E(1), and E(2)** attached hereto.

54. This initial demand immediately triggered investigative efforts by Onsite.

55. Indeed, Onsite commenced its "URGENT" response efforts that same day. *See, e.g.,* **Exhibit F** attached hereto.

56. By the following day, April 12, 2014, Safeway had followed up in writing to Onsite relaying iSight's assessment the scope of the breach potentially extended to *all* Onsite's customers (past and present), i.e., "Entities that *are or have been customers* of Onsite . . . should

be aware that the personal information of some of their employees has *almost certainly* been compromised." *See* **Exhibit G** attached hereto (emphasis added).

57. Safeway further relayed its expectation remedial action was needed based on the following warning in the iSight report: "Safeway is a client of Onsite . . . . A purchaser [of the stolen data] could use the records in the database (and the screening results that could likely be obtained via the login information) in support of a variety of malicious activities, such as *targeted phishing attacks, insurance fraud and identity theft*." *See id*. (emphasis added).

58. Onsite's preliminary efforts to respond to these threats led to additional written demands from still other Onsite customers and affected persons, with escalating urgency for a comprehensive remedial response.

59. By way of example, from April 2014 through in or about July 2014, Onsite received written demands from customers or third-party companies to whom Onsite provided screening services, all demanding remedial action. *See, e.g.,* **Exhibits H – P** attached hereto.

60. The customers and companies included, but were not necessarily limited to, Allstate, Conoco, Family Dollar, Healthways, Ingersoll Rand, Phillips 66, and WedMD. *Id*.

E. Onsite's Remedial Actions

61. In response to Safeway's first written demand for a remedy on April 11, 2014, and to respond to the subsequent demands referenced above—Onsite undertook three principal steps based on its legal duties to remedy the Data Breach without delay and mitigate against even greater losses.

62. It retained:

- Stroz Friedberg to "confirm that the Scheduler Database was compromised; 2) confirm the method of compromise; and 3) determine, to

the extent possible, what tables in the Scheduler Database were opened, copied, manipulated, or downloaded." **Exhibit D** attached hereto.

- The law firm Haynes & Boone to in pertinent part instruct Onsite regarding time-sensitive and mandatory remedial steps, as well as distinct guidance Haynes & Boone provided regarding certain legal "notification" obligations, and
- the security firm ID Experts to facilitate the Data Breach remedy by providing credit monitoring and identity protection services to the individuals whose Personal Data was stolen or at risk of having been stolen.

63. These remedial steps began in April 2014, *after* Onsite received the initial Safeway demand on April 11th, and continued through approximately December 2014.

64. As a result of the steps, Onsite determined Personal Data associated with Safeway perhaps had not been compromised because that data was stored on New Scheduler (for which there was no evidence of a breach)—but as iSight initially cautioned, and as Stroz Friedberg confirmed, Personal Data for customers and third parties that had been stored on Old Scheduler and Backup Scheduler indeed was compromised and stolen.

65. Onsite collectively has incurred well in in excess of $1,000,000.00 in damages within the meaning of NetProtect Policy Section VI, Professional Liability Policy Section V(6), and Umbrella Policy Section VI(34), to facilitate the remedial response and correct the data theft.

66. Onsite further has incurred damages within the meaning of the Polices in the form of customer "credits."

67. Had Onsite failed to undertake the remedial steps in the prompt manner it did—by instead "stonewalling" its customers and third persons regarding the verified Data Breach—the risk of "targeted phishing attacks, insurance fraud and identity theft" would have increased in scale, as would the derivative financial liabilities for which Onsite would have been responsible.

F. The NetProtect Policy and American Casualty's Insufficient Coverage Position

68. NetProtect Policy coverage I(A)(1) covers the time period inclusive of the March 2014 Data Breach and indemnifies up to $1,000,000.00 for Onsite's "'damages' as a result of a 'wrongful act' that results in a 'claim' alleging *'network damage,'* violation of any 'security breach notice law' or 'privacy injury and identity theft . . . .'" (emphasis added).

69. Policy Section VI defines a triggering "claim" to include: "a written demand for monetary *or* non-monetary relief . . . ." (emphasis added).

70. The Policy further recognizes an underlying event that triggers multiple demands operates as a single, undifferentiated basis for a "claim."

71. Policy Section I(A)(4) provides, for instance: "More than one 'claim' involving the same 'wrongful act' or 'related wrongful acts' shall be considered as one 'claim' which shall be deemed made on the earlier of . . . the date on which the *earliest* such 'claim' was first made . . . ." (emphasis added).

72. Additional context is provided by Policy Section VI, which provides: "'Related wrongful act' mean [sic] all 'wrongful acts' that are temporally, logically or causally connected by any common fact, circumstance, situation, transaction, event, advice or decision."

73. Further context is evident in the portion of Policy Section VI that defines "Related claims" to "mean all 'claims' based on or arising out of a single 'wrongful act' or any 'related wrongful acts.'"

74. The "vulnerability" in Onsite's network, which failed to prevent the Data Breach—and led to all claims, was a "wrongful act" within the meaning of coverage I(A)(1), because Policy Section VI defines an act of the kind as "any actual or alleged error, omission, neglect or breach of duty that results in a 'security breach.'"

75. A "security breach" indeed occurred in or about March 2014, because within the meaning of Policy Section VI, the vulnerability in Onsite's network prevented the network from "identify[ing] and authenticat[ing] parties prior to accessing [Onsite's] network" and otherwise prevented the network from "control[ing] access to [Onsite's] network and monitor[ing] and audit[ing] such access . . . ."

76. That breach moreover caused "network damage," defined in Policy Section VI to include, *inter alia*: "electronic information damage or *theft* . . . ." (emphasis added).

77. American Casualty has *admitted* it received notice of these coverage-triggering events by no later than September 2014—during the NetProtect Policy coverage period. *See* **Exhibit Q** attached hereto.

78. Indeed, either directly, or in connection with associated insurers (including Defendant Columbia Casualty) who collectively operate under the banner "CNA," American Casualty actively injected itself in the breach investigation by no later than *July* 2014.

79. By way of example, after Stroz Friedberg prepared its initial Report in June 2014, "CNA" coordinated with Onsite to obtain additional information from Stroz Friedberg regarding the Data Breach, because in a follow-up report dated July 24, 2014, Stroz Friedberg noted: "*At the request of CNA Insurance*, and at the direction of counsel for Onsite . . ., Stroz Friedberg was tasked to provide *additional* information regarding the compromise of [Onsite]'s Scheduler application . . . by a malicious attacker." **Exhibit R** attached hereto (emphasis added).

80. Notwithstanding American Casualty's active investigation of the Data Breach by no later than July 2014, and formal acknowledgment of notice at least by September 2014, American Casualty did not address or take a position *of any kind* on the NetProtect Policy Section I(A)(1) coverage until February 8, 2016—approximately a year-and-a-half later. *See* **Exhibit Q** attached hereto.

81. Even in that belated communication, American Casualty did not articulate a coherent position regarding Onsite's right to coverage under NetProtect Policy Section I(A)(1).

82. It instead took what at best are internally conflicting coverage positions.

83. In one respect, American Casualty assented to the findings made in the Stroz Report:

> The Stroz Report *confirmed* that both an [Onsite] Original Scheduler server and a Backup Scheduler Server were compromised . . . and the main attack vector was a Struts *vulnerability* that the attacker exploited in order to allow for the remote issuance of commands on the servers. The Stroz Reported [sic] noted there is strong evidence to suggest that the 'user' table in the Scheduler Database was targeted by the attacker and although it did not identify direct forensics evidence to support a conclusion that the table was copied and/or exfiltrated by the attacker, there was compelling circumstantial evidence to support such a conclusion.

Exhibit Q (emphasis added).

84. Consistent with these acknowledgments, American Casualty (eventually) recognized its duty to provide a defense under the NetProtect Policy with respect to a legal cause of action brought by an adversely affected Onsite customer, Virgin Healthmiles, Inc.

85. American Casualty also made partial indemnification for Policy Section I(A)(1) "damages," regarding Onsite's payment of losses upon the demand of Onsite customer Staywell, Inc.

86. American Casualty moreover exhausted a $25,000.00 "sublimit" (*not at issue in this lawsuit*) under the NetProtect Policy related to "Supplementary Payments for Regulatory Expenses" insured under discrete Policy Section I(A)(2)—which (notably) shares in common the same basic coverage-triggering events that herein mandate coverage under Section I(A)(1).

87. But American Casualty has not otherwise taken a coherent or credible position on coverage regarding the *remaining* damages Onsite suffered within the meaning of Policy Section I(A)(1), nor has American Casualty exhausted the $1,000,000.00 limit of liability although Onsite's damages exceed that limit.

88. American Casualty instead refuses to acknowledge or pay these covered losses and has not otherwise complied with its statutory duties under Chapter 542 of the Texas Insurance Code.

G. The Professional Liability and Umbrella Policies, and Columbia Casualty's Improper Coverage Denial

89. The Professional Liability Policy also covers the time period inclusive of the Data Breach and indemnifies up to $1,000,000.00 for "all amounts . . . which [Onsite] becomes legally obligated to pay as 'damages' as a result of a 'claim' *or* 'circumstance' arising from an act, error or omission in the *rendering* of 'professional services' . . . ." (emphasis added).

90. The Umbrella Policy provides an additional $1,000,000.00 excess coverage under materially identical terms.

91. The respective Policies define a "claim" to include any "written or oral demand . . . .," which further is defined to mean "a written or oral demand for money *or* services, which is *not* a 'suit', received by [Onsite], arising out of an act, error or omission in the *rendering* of 'professional services'." (emphasis added).

92. A "circumstance" moreover includes "an act, error or omission from which [Onsite] reasonably expect[ed] that a 'claim' could be made . . . ."

93. Damages are defined to include "settlements [Onsite was] legally obligated to pay because of a covered 'claim' *or* 'circumstance' . . . ." (emphasis added).

94. The "professional services" covered under the Professional Liability Policy and Umbrellas Policy could be in the form of "administrative services," defined as any activity qualifying as "planning, organizing, directing and controlling [Onsite's] business operations."

95. Covered "professional services" also could be in the form of "medical laboratory services," defined to include "the *collection* or testing of materials from the human body for the purpose of:

a. providing information for the *diagnosis, prevention, or treatment* of any disease or impairment, or

b. *assessing* the health of human beings." (emphasis added).

96. Medical laboratory services alternatively were defined to include "the *provision* of materials derived from the human body to a laboratory so that such laboratory [could]:

a. provide information for the diagnosis, prevention, or treatment of any disease or impairment, or

b. assess the health of human beings . . . ." (emphasis added).

97. All of the Personal Data that was compromised during the Data Breach was amassed through Onsite's "rendering" of professional services as defined under *both* the "administrative services" criterion and "medical laboratory services" criterion.

98. With respect to the former, in order for Onsite to "render" its healthcare screening services, it was essential for it to safely and securely "organize," "direct" and otherwise "control"

the Personal Data that was acquired as the essential condition of Onsite's health screening "business operations."

99. The errors and omissions with Onsite's network (characterized as the "vulnerability" by Stroz Friedberg), nevertheless allowed unauthorized access to the information, and triggered the remedial costs Onsite seeks to recover as damages in this lawsuit.

100. Likewise, *all* of the Personal Data Onsite amassed and stored was accumulated for Onsite to render its core service of "collecting" materials to facilitate diagnostic, preventive, treatment, or healthcare assessments for screening participants, and in other instances to "provide" the necessary material to laboratories for those purposes.

101. Columbia Casualty has admitted it received notice of Onsite's claims under both the Professional Liability Policy and Umbrella Policy, but notwithstanding the clear grounds for coverage as pleaded herein, Columbia Casualty declined to provide coverage by letter dated June 15, 2015. *See* **Exhibit S** attached hereto.

102. Columbia Casualty rationalized the denial first by proffering what is plainly an inaccurate reading of the two policies, because Columbia Casualty contended coverage was lacking unless a "claim or suit has been *filed* . . . ." (emphasis added).

103. As pleaded herein, the Professional Liability and Umbrella Policies state expressly that coverage attaches in the event of "a written or oral demand for money or services, which is *not* a 'suit' . . . ." (emphasis added).

104. There consequentially is no basis under either policy for Columbia Casualty's assertion something needed to be "filed" before Columbia Casualty's indemnity obligations were triggered.

105. Columbia Casualty further attempted to justify its coverage denial by summarily asserting: "We also do not believe [Onsite] was rendering a 'professional service' as defined in the Policy at the time of the Data Breach."

106. Columbia Casualty proffered no good faith reading of the Professional Liability or Umbrella Policy terms, as pleaded and incorporated herein, that could support that assertion.

107. Columbia Casualty finally purported to disclaim coverage premised on its suggestion Onsite did not have "consent" from Columbia Casualty to resolve the harms and losses caused by the Data Breach.

108. That assertion is inconsistent with Columbia Casualty's (through CNA's) first-hand involvement in the initial remedial investigation as early as July 2014.

109. The assertion further was made without any suggestion how Columbia Casualty contends it was "prejudiced" by the damages Onsite incurred to mitigate the magnitude of escalating liabilities plainly covered by the Professional Liability and Umbrella Policies and that already had manifest by April 2014.

CLAIMS FOR RELIEF

Count I – Breach of Contract (American Casualty)

110. Paragraphs 1 through 109 are incorporated herein by reference.

111. The NetProtect Policy was a valid and enforceable contract of insurance, pursuant to which Onsite fulfilled all applicable duties, including, but not necessarily limited to, payment of premiums and provision of notice and documentation of claims to American Casualty.

112. To the extent, if at all, Onsite was not in technical compliance with any term or condition under the NetProtect Policy, American Casualty was not thereby prejudiced.

113. For instance, Onsite's prompt and diligent remedial responses to the Data Breach fulfilled clear legal duties and mitigated against even greater, covered losses.

114. American Casualty nonetheless has failed to fulfill its duty to indemnify Onsite as required by the NetProtect Policy, which has caused Onsite contractual damages sought herein.

WHEREFORE, Plaintiff Onsite Health Diagnostics, LLC respectfully requests this Honorable Court: (1) enter declaratory judgment, pursuant to 28 U.S.C. § 2201, declaring Defendant American Casualty Company of Reading, PA liable for all unexhausted amounts owed under Network Security, Privacy & Identity Theft Liability Policy No. 4031611691; (2) enter judgment awarding breach of contract damages against American Casualty; (3) award pre-judgment and post-judgment interest as allowed by Chapter 542 of the Texas Insurance Code, or as otherwise allowed by law; (4) award Onsite its litigation attorneys' fees as allowed by Chapter 542 of the Texas Insurance Code, or as otherwise allowed by law; and (5) grant Onsite all other relief, at law or in equity, to which it may be entitled.

Count II – Breach of Contract (Columbia Casualty)

115. Paragraphs 1 through 109 are incorporated herein by reference.

116. The Professional Liability and Umbrella Policies were valid and enforceable contracts of insurance, pursuant to which Onsite fulfilled all applicable duties, including, but not necessarily limited to, payment of premiums and provision of notice and documentation of claims to Columbia Casualty.

117. To the extent, if at all, Onsite was not in technical compliance with any term or condition under the respective policies, Columbia Casualty was not thereby prejudiced.

118. For instance, Onsite's prompt and diligent remedial responses to the Data Breach fulfilled clear legal duties and mitigated against even greater, covered losses.

119. Columbia Casualty nonetheless has failed to fulfill its duty to indemnify Onsite as required by the Professional Liability and Umbrella Policies, which has caused Onsite contractual damages sought herein.

WHEREFORE, Plaintiff Onsite Health Diagnostics, LLC respectfully requests this Honorable Court: (1) enter declaratory judgment, pursuant to 28 U.S.C. § 2201, declaring Defendant Columbia Casualty Company liable for all unexhausted amounts owed under Healthcare Facilities Professional Liability Coverage Form – Claims Made Policy No. HMA 4031930279-2 and Healthcare Facilities Umbrella Policy No. HMC 4031936700-2; (2) enter judgment awarding breach of contract damages against Columbia Casualty; (3) award pre-judgment and post-judgment interest as allowed by Chapter 542 of the Texas Insurance Code, or as otherwise allowed by law; (4) award Onsite its litigation attorneys' fees as allowed by Chapter 542 of the Texas Insurance Code, or as otherwise allowed by law; and (5) grant Onsite all other relief, at law or in equity, to which it may be entitled.

Count III – Chapter 542 Violations (American Casualty)

120. Paragraphs 1 through 109 are incorporated herein by reference.

121. American Casualty engaged in the business of insurance in Texas by virtue of its authority to issue, and its actual issuance of the NetProtect Policy.

122. American Casualty nevertheless violated each of the following proscriptions in Texas Insurance Code section 542.003, at minimum, by delaying at least sixteen months to formally respond to Onsite's claim and thereafter failing to fully indemnify Onsite notwithstanding the facts clearly establishing coverage—all of which constitute failures in violation of:

- section 542.003(b)(2), to acknowledge with reasonable promptness Onsite's pertinent communications relating to Onsite's claim arising under the NetProtect Policy;
- section 542.003(b)(3), to adopt and implement reasonable standards for the prompt investigation of claims such as Onsite's under the NetProtect Policy;

- section 542.003(b)(4), to in good faith effect a prompt, fair, and equitable settlement of Onsite's claim although liability has been reasonably clear; and
- section 542.003(b)(5), to save Onsite from instituting suit to recover outstanding amounts due under the NetProtect Policy, because American Casualty has offered substantially less than the amount to which Onsite shall prove itself entitled.

123. American Casualty moreover violated Texas Insurance Code section 542.056, at minimum, by failing in violation of:

- section 542.056(a), to notify Onsite in writing of the acceptance or rejection of Onsite's claim not later than the 15th business day after American Casualty received all items, statements, and forms required to secure final proof of loss;
- section 542.056(d), to notify Onsite that American Casualty was unable to accept or reject the claim or why American Casualty could not do so not later than the 15th business day after Onsite submitted its claim; and
- section 542.056(d), by otherwise failing to accept or reject Onsite's claim not later than the 45th day of American Casualty's statutory triggers to do so.

WHEREFORE, Plaintiff Onsite Health Diagnostics, LLC respectfully requests this Honorable Court: (1) award damages against Defendant American Casualty Company of Reading, PA as allowed by Texas Insurance Code sections 542.058 and 542.060; (2) award pre-judgment and post-judgment interest as allowed by Texas Insurance Code section 542.060, or as otherwise allowed by law; (3) award Onsite its litigation attorneys' fees as allowed by Texas Insurance Code section 542.060, or as otherwise allowed by law; and (4) grant Onsite all other relief, at law or in equity, to which it may be entitled.

Count IV – Chapter 542 Violation (Columbia Casualty)

124. Paragraphs 1 through 109 are incorporated herein by reference.

125. Columbia Casualty engaged in the business of insurance in Texas by issuing the surplus lines of insurance provided by the Professional Liability Policy and Umbrella Policy, to a Texas insured, pursuant to Texas law.

126. Columbia Casualty nevertheless violated, at minimum, the following proscriptions in Texas Insurance Code section 542.003, by not attempting, in violation of section 542.003(b)(4), to in good faith effect a prompt, fair, and equitable settlement of Onsite's claim although liability has been reasonably clear.

WHEREFORE, Plaintiff Onsite Health Diagnostics, LLC respectfully requests this Honorable Court: (1) award damages against Defendant Columbia Casualty Company as allowed by Texas Insurance Code sections 542.058 and 542.060; (2) award pre-judgment and post-judgment interest as allowed by Texas Insurance Code section 542.060, or as otherwise allowed by law; (3) award Onsite its litigation attorneys' fees as allowed by Texas Insurance Code section 542.060, or as otherwise allowed by law; and (4) grant Onsite all other relief, at law or in equity, to which it may be entitled.

JURY DEMAND

Onsite hereby requests a jury trial on all issues so triable.

October 20, 2017

Respectfully submitted,

s/ Nolan C. Knight
Nolan C. Knight
TX Bar No. 24027125
E-mail: nknight@munsch.com
MUNSCH HARDT KOPF & HARR, P.C.
3800 Ross Tower
500 North Akard St.
Dallas, Texas 75201
Telephone: (214) 855-7500
Facsimile: (214) 855-7584

Michael E. Coles
TX Bar No. 24007025
E-mail: mikec@colesfirm.com
THE COLES FIRM
4925 Greenville Ave., Ste. 200
Dallas, TX 75206-4035
Telephone: (214) 443-7862
Facsimile: (214) 718-0480

COUNSEL FOR PLAINTIFF
ONSITE HEALTH DIAGNOSTICS, LLC